UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,426	09/22/2000	Alexander Medvinsky	18926-004600US	1955

20350 7590 07/16/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/668,426	MEDVINSKY, ALEXANDER	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) *19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14-18,20 and 21* is/are rejected.

7)☐ Claim(s) *13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in the application.

2. Claims 1-12, 14-18, 20 and 21 stand being rejected.

3. Claim 19 has been cancelled.

4. Claim 13 has been objected to.

Response to Arguments

5. Applicant's arguments with respect to claims 1-11, 18, 20 and 21 have been considered but are moot in view of the new ground(s) of rejection.

6. With respect to claims 12-17, applicant's arguments filed 4/28/04 have been fully considered but they are not persuasive.

With regard to claim 12, the applicant argues, on page 9, that Brown fails to teach a CTA (cable telephony adapter).

The examiner respectfully disagrees. The network as taught by Brown is a telephone network. Therefore, the telephone network is going to contain a CTA for secure transactions.

With regard to claim 14, the applicant argues, on page 9, that Brown fails to teach "receiving an AP request message from said client". The applicant argues that Brown fails to teach the element "transmitting said nonce coupled with said trigger message to said CTA".

The examiner respectfully disagrees. With respect to the request message, Brown teaches it. The request message would have been the challenge message. As far as the element "transmitting said nonce coupled with said trigger message to said CTA", the examiner asserts that it is not a limitation in claim 14.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 12-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Brown U.S. Patent No. 6,058,480.

As to claim 12, Brown discloses providing the Signaling Controller. Brown discloses providing the CTA configured to be coupled to the Signaling Controller. Brown discloses providing a key distribution center (KDC) [column 6, lines 33-67]. Brown discloses generating a trigger message at the Signaling Controller. Brown discloses generating a nonce at the Signaling Controller. Brown discloses coupling the nonce with the trigger message. Brown discloses transmitting the nonce coupled with the trigger message to the CTA [column 9, lines 11-27]. Brown discloses generating a response message to the trigger message. Brown discloses using the value of the nonce as the value of a returned nonce. Brown discloses coupling the response message with

the returned nonce. Brown discloses transmitting the returned nonce and the response message to the Signaling Controller [column 10, lines 27-30]. Brown discloses comparing the returned nonce to the nonce. Brown discloses transmitting an All reply in reply to the response message. Brown discloses transmitting an SA recovered message to the Signaling Controller [column 10, lines 31-37].

As to claim 13, Brown discloses generating a wakeup message at the server. Brown discloses generating a server nonce at the server. Brown discloses conveying the wakeup message and the nonce to the client [column 9, lines 11-27]. Brown discloses generating an All request message at the client. Brown discloses conveying a client-nonce and the All request message to the server [column 10, lines 27-30]. Brown discloses confirming that the client nonce conveyed with the All request message matches the server nonce generated at the server [column 10, lines 31-37].

As to claim 14, Brown discloses receiving an All request message from the client. Brown discloses receiving a client nonce from the client wherein the client nonce is associated with the All request. Brown discloses determining whether the client nonce matches a nonce conveyed from the server [column 10, lines 11-37].

As to claim 15, Brown suggests determining that the client nonce does not match the nonce conveyed from the server. Brown suggests disregarding the All request [column 10, lines 11-37].

As to claim 16, Brown discloses awaiting at the client for a reply from the server to the AP request. Brown discloses aborting the AP request session after a predetermined time period if no reply is received from the server [column 20, lines 31-44].

As to claim 17, Brown discloses determining that the client nonce does match the nonce conveyed from the server. Brown discloses generating an AP reply at the server to the AP request [column 21, lines 26-33].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-11, 18, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown U.S. Patent No. 6,058,480 in view of Dice U.S. Patent No. 6,289,451 B1.

As to claims 1, 7 and 18, Brown discloses providing a server. Brown discloses providing a client configured to be coupled to the server. Brown discloses providing a trusted third party configured to be coupled to the client [column 6, lines 33-67]. Brown discloses generating a trigger message at the server. Brown discloses generating a nonce at the server. Brown discloses allowing the server to initiate a key management session with the client. Brown discloses utilizing the nonce coupled with the trigger message [column 9, lines 11-27].

Brown does not teach coupling the nonce with the trigger message.

Dice teaches coupling a nonce with a message [column 11, lines 1-13].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown so that the nonce was coupled with the trigger message.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Brown by the teaching of Dice because it reduces the computation load of engaging in a communication session by reducing the amount of encryption and decryption that is required, allowing for minimal latency and the use of lower-cost communication devices in the system. Since the invention requires encryption and decryption only of the session key, an encryption and decryption operation is required only once or only a relatively small number of times during the communication session, to ensure privacy of the session key value, not each time a message packet is transferred [column 10, lines 33-43].

As to claims 2 and 8, Brown teaches that allowing the server to initiate the key management session with the client comprises conveying the trigger message and the nonce to the client [column 9, lines 11-14].

As to claims 3, 9 and 20, Brown teaches receiving the trigger message and the nonce at the client. Brown teaches generating a response message to the trigger message. Brown teaches conveying the response message and a returned nonce to the server [column 10, lines 27-30].

As to claim 4, Brown teaches an out-of-bounds value for the nonce to prevent an attacker from simulating a client initiated key management session. Brown teaches checking the nonce to determine whether the value of the nonce is the out-of-bounds value [column 11, lines 9-21].

As to claims 5, 10 and 21, Brown teaches confirming the value of the returned nonce at the server. Brown teaches conveying a reply message from the client to the server [column 10, lines 31-37].

As to claims 6 and 11, Brown teaches receiving from the client a response message and a false nonce at the server. Brown teaches determining that the false nonce is false. Brown teaches disregarding the client response message. Brown teaches determining that the server did not initiate the key management session [column 14, lines 51-67].

Allowable Subject Matter

9. Claim 13 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 13, the examiner withdraws the rejection of the claim. Neither Brown nor prior art teaches generating a wakeup message at the server and conveying the message with a nonce to the client.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the

advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
July 9, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100